PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Piwonka, et al.	)	Examiner: V. Perungavoor
	)	Art Unit: 2132
Serial No.: 10/821,746	)	
Filed: 04/09/2004	)	
For: SYSTEMS AND METHODS FOR SECURING PORTS	)	
Date of Final Office Action: April 3, 2008	)	Attorney Docket No.: 200313976-1
Notice of Appeal Filed: June 30, 2008	)	

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This Appeal Brief is timely provided to support the Notice of Appeal filed June 30, 2008.

1. Real Party in Interest:

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

2. Related Appeals and Interferences

There are no other prior and/or pending appeals, interferences, or judicial proceedings that are related to, directly affect, or that will be directly affected by or have a bearing on the Board's decision.

3. Status of Claims

Claims 1-30 are pending in the application.

Claims 1-30 stand rejected.

No claims were canceled.

No claims were allowed.

No claims were withdrawn

The rejections of claims 1-30 are appealed.

4. Status of Amendments

No Amendments were filed subsequent to the Final Office Action.

5. Summary of Claimed Subject Matter

Independent Claim 1

Claim 1 recites a system for securing one or more ports of a computing device that includes an actual number of physical ports and a data store that contains a port count specifying the actual number of physical ports (spec. page 5, [0024] lines 1-2; and [0025] lines 1-5). The system comprises a configuration logic configured to provide a security option for securing one or more selected ports (spec. page 6, [0026] lines 6-8; figure 1, port security logic 110, fig. 2 configuration logic 220).

A security logic is configured to, in response to the security option being selected, cause the data store to be modified by changing the port count to specify a fewer number of physical ports to cause an operating system to not detect the one or more selected ports (spec. page 6, [0026] lines 1-5; fig. 1 port security logic 110, data store 115).

Independent Claim 10

Claim 10 recites a computing system (fig. 1, device 100, fig. 7, computer 700) that comprises a housing (fig. 1, housing 105), one or more processors (fig. 7, processor 702), and a set of physical ports (fig. 1, e.g. ports 1-6). The physical ports include one or more front ports positioned on the housing and being accessible by a user to connect an external device to the computing system. The ports also include one or more back ports, positioned on the housing, being configured to connect an external device to the computing system (spec. page 6, lines 1-5).

The computing system also includes a structural parameter (fig. 2, structural parameters 205) configured to indicate a total number of physical ports (fig. 2,

number of port 210) that are present in the computing system including the one or more front ports and the one or more back ports (spec. page 7, [0028] lines 4-7; fig. 2, parameters 205 and number of ports 210). The structural parameter is configured to indicate a fewer number of ports than the total number of physical ports in order to prohibit operation of the one or more front ports (spec. page 6, [0025] lines 7-12, and [0026]).

The computing system includes an operating system configured to enumerate ports that are present in the computing system based on the structural parameter. The structural parameter causes the one or more front ports to be undetectable by the operating system causing the one or more front ports to be inoperable (spec. page 7, [0028] lines 9-10; page 8, lines 1-5).

Independent Claim 16

Claim 16 recites a method for securing a port in a device having a total number of physical ports (spec. page 12, [0040] lines 1-2; fig. 4). The method comprises receiving a signal that indicates a number of ports to be secured from user access (spec. page 12, [0040] lines 4-6; fig. 4 block 405). A data store is accessed that contains a value for the total number of physical ports (spec. page 12, [0041] lines 2-3; fig. 4 block 410). The value in the data store is then reduced by the number of ports to be secured to cause an operating system to be aware of a number of physical ports that is less than the total number of physical ports (spec. page 12, [0041] lines 3-9; fig. 4 block 415).

Independent Claim 21

Claim 21 recites a computer-readable medium for providing processor executable instructions operable to perform a method (spec. page 13, [0045] lines 1-4). The method comprises providing a security option to secure one or more ports of a device (spec. page 13, [0047] lines 1-3; fig. 5 block 515). In response to the security option being selected for a port, a reduced number of physical ports is

specified that is less than an actual number of physical ports present in the device (spec. page 14, [0048] lines 1-4). The method also recites changing a configuration parameter that indicates, to an operating system, the actual number physical ports, where the configuration parameter is changed to indicate the reduced number of physical ports causing the operating system not to enumerate the one or more ports (spec. page 14, [0048] lines 4-8, and [0049] lines 1-2).

Independent Claim 25

Claim 25 recites a system comprising port configuration means for selecting a port to be secured from a set of physical ports configured within a computing device. One structure that corresponds to the claimed function of selecting a port is a computing device with a graphical user interface (see specification page 13, lines 16-28, or [0045-0046]).

Claim 25 also recites security means for causing an operating system to not enumerate the selected port to cause the selected port to be inoperable, including modifying a port count to specify one less port than a total number of the set of physical ports where the operating system enumerates ports based on the port count. One structure that corresponds to the claimed function of causing and modifying a port count includes port security logic 110 (spec. page 6, [0026] lines 1-5; fig. 1 port security logic 110). Logic is defined to include hardware, firmware, software and/or combinations of each (spec. page 3, [0016]).

Independent Claim 27

Claim 27 recites a method in a computer system having a graphical user interface comprising a display and a selection device, a method of providing and selecting from a set of data entries on the display (specification page 13, lines 16-28, or [0045-0046]). The method comprises retrieving a one or more data entries, where a data entry represents a security status of a port (specification page 13, line

31 to page 14, line 1). The one or more data entries are displayed on the display to show the security status and allow the security status to be modified (specification page 13, lines 29-31). The method includes receiving a data entry selection signal indicative of the selection device selecting one or more of the data entries that modifies the security status of a port (specification page 14, lines 5-9).

In response to the data entry selection signal, initiating an operation that causes a configuration parameter to be modified in accordance with the security status where the configuration parameter stores a value that specifies a total number of physical ports that are present in the computer system. The operation causes the value to be reduced in response to the security status for a selected port being set to indicate a secured status to cause an operating system not to enumerate the selected port (specification page 14, lines 10-22).

6. Grounds of Rejection to be Reviewed on Appeal

I. Whether claims 1-9, 21-26 are unpatentable under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter.

II. Whether claims 1-3, 5-7, 9-12, 15-18, 21-28 are unpatentable under 35 U.S.C. 102(e) as being anticipated by Thayer (U.S. Pub. No. 2002/0116604 A1).

III. Whether claims 4, 8, 13-14, 19, 24, 29-30 are unpatentable under 35 U.S.C. §103(a) as being obvious over Thayer, in view of Zimmer et al. (US Patent Publication 2005/0010811).

7. Argument

I. Whether claims 1-9, 21-26 are unpatentable under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter.

Appellant notes that no authority to support the rejection was provided in the Office Action (see pages 2-3). Rejections must be based on substantive law. MPEP 2107, I, first paragraph states, "Rejections will be based upon the substantive law..." No substantive law has been cited in the Office Action to support the §101 rejections and the rejections cannot stand for this reason alone.

MPEP 2106 "Patent Subject Matter Eligibility" requires in section VII:

VII. CLEARLY COMMUNICATE FINDINGS, CONCLUSIONS AND THEIR BASES

> Once USPTO personnel have concluded the above analyses of the claimed invention under all the statutory provisions, including **35 U.S.C. 101, 112, 102** and **103**, they should review all the proposed rejections and their bases to confirm that they are able to set forth a *prima facie* case of unpatentability. Only then should any rejection be imposed in an Office action. The Office action should clearly communicate the findings, conclusions and reasons which support them.

The Office Action has not clearly communicated the findings, conclusions or reasons which support the rejection. Only conclusory statements were provided.

Independent Claim 1

The examiner's reasoning appears to be that since claim 1 includes a logic that may include a software element, it is per se non statutory. No findings, reasons, or laws were provided in the Office Action to support the conclusion.

MPEP 2106 section IV "DETERMINE WHETHER THE CLAIMED INVENTION COMPLIES WITH 35 U.S.C. §101, (A), paragraph 7, states:

> The subject matter courts have found to be outside of, or exceptions to, the four statutory categories of invention is limited to abstract ideas, laws of nature and natural phenomena.

Claim 1 recites a system for securing ports of a computing device and comprises configuration logic and security logic. No part of claim 1 is an abstract idea, law of nature or natural phenomena. Claim 1 is thus statutory subject matter and the rejection should be reversed.

MPEP 2106, section IV(C) also lists a series of tests that the examiner should complete prior to rejecting a claim under §101 as stated in MPEP 2106 IV(D). Performing those tests shows that the present claims are statutory subject matter.

For example, claim 1 provides a practical application that produces a useful, concrete, and tangible result. The system of claim 1 is useful because it allows one or more ports on a computing device to be secured where a port is not detected by an operating system and thus cannot be used (see specification, paragraph [0024]). The system of claim 1 also provides a concrete and tangible result, for example, by changing a port count to specify a fewer number of physical ports. This feature is also a physical transformation since the system changes a port count. Therefore, claim 1 recites statutory subject matter and the rejection should be reversed.

Independent Claim 21

Independent Claim 21 recites "[a] computer-readable medium for providing processor executable instructions operable to perform a method." This is a standard Beauregard-type claim that has been ruled to be statutory subject matter.

In re Beauregard, 35 USPQ2d 1383 (Fed. Cir. 1995). MPEP 2106.01 also states that this claim type is statutory:

> MPEP 2106.01, Section I, paragraph 2, states:
>
> "In contrast, a claimed computer-readable medium encoded with a computer program is a computer element which defines structural and functional interrelationships between the computer program and the rest of the computer which permit the computer program's functionality to be realized, and is thus statutory. See *Lowry*, 32 F.3d at 1583-84, 32 USPQ2d at 1035." (emphasis added)

Therefore, the present rejection is contrary to the MPEP and case law. Claim 21 also provides a practical application that produces a useful, concrete, and tangible result similar to claim 1. Claim 21 is useful because it provides for securing ports of a device. The system of claim 21 also provides a concrete and tangible result, for example, by changing a configuration parameter. This feature is also a physical transformation since a parameter is changed. Therefore, claim 21 recites statutory subject matter and the rejection should be reversed.

Appellant notes that the definition of "computer-readable medium" in paragraph [0014] of the present specification was amended in the response filed January 25, 2008.

Independent Claim 25

Claim 25 is a standard means-plus-function claim allowed by statute (35 U.S.C. §112, 6th paragraph). Claim 25 is similar to claim 1 and recites statutory subject matter for similar reasons. The rejection should be reversed.

II. Whether claims 1-3, 5-7, 9-12, 15-18, 21-28 are unpatentable under 35 U.S.C. 102(e) as being anticipated by Thayer (U.S. Pub. No. 2002/0116604 A1).

Independent Claim 1

Claim 1 is directed to a system for securing ports. The claim recites:

> a security logic configured to, in response to the security option being selected, cause the data store to be modified by changing the port count to specify a fewer number of physical ports to cause an operating system to not detect the one or more selected ports.

Thayer does not disclose any of these features. In general, Thayer is directed to "enabling" a hidden port that makes the hidden port usable. The Summary of the Invention states:

> [0015] A method, system, apparatus, and computer program product are presented for enabling a hidden port in a computing device. ... the computing device is configured to use the hidden port for general I/O purposes...
>
> Thayer, page 2, paragraph [0015], lines 1-9; (emphasis added)

Enabling a port is an opposite function from "securing" a port, which is what the present claims are directed to. Hence, Thayer is not relevant to the present subject matter and fails to anticipate any of the present claims.

In particular, the Office Action relies on Thayer paragraphs [0057-0061] as teaching "...causes the data store to be modified by changing the port count to specify a fewer number of physical ports..." (Final Office Action, page 3, 3rd paragraph). Nothing in the cited paragraphs has any relevance to changing port counts and the paragraphs fail to teach or suggest the claimed feature. For example, paragraph [0057] merely lists to the reader a set of terms "used herein"

for explanation. Nothing teaches a logic that changes a port count. Paragraphs [0058-0059] merely recite physical requirements of a "debug port." Nothing teaches a logic that changes a port count. Paragraph [0060] merely gives a definition of a "hidden port", which is a port within a device and not externally accessible. Again, nothing teaches a logic that changes a port count. Lastly, paragraph [0061] simply explains the advantage of its invention, which is to allow a user to use an internally hidden debug port.

Thus nothing in the cited paragraphs teaches logic configured to "cause the data store to be modified by changing the port count to specify a fewer number of physical ports." Claim 1 is not anticipated and Thayer fails to establish a prima facie anticipation rejection. The rejection is improper and should be reversed. Accordingly, the rejections of dependent claims 2-9 are also improper and should be reversed. All claims should now be allowed.

Additionally, the Office Action at the bottom of page 3 cites Thayer [0049-0050] as relating to port counts and hiding selected ports. The Office Action is incorrect. Paragraph [0049] discusses enabling a hidden port for use and that a hidden port is "configured for general purpose use". Paragraph [0050] discusses how to configure a computer to use the debug serial port by copying the address of the debug serial port to a memory location. Both paragraphs discuss making a port usable. Thus, neither paragraph [0049] or [0050] teach changing port counts, making ports undetectable, or otherwise anything about securing a port. No claim is anticipated by these paragraphs.

Claim 1 also recites "...to cause an operating system to not detect the one or more selected ports." This is contrary to the operation of Thayer. Thayer is directed to making an internal port usable. To be usable, Thayer teaches that the port must be "detected" (Thayer, page 5, [0051] lines 4-5: "Assuming that a hidden port is present on a system and has been detected..."). Again, the reliance on

Thayer is misguided and Thayer fails to teach or suggest any claim. A prima facie rejection has not been established and all rejections should be reversed.

Independent Claim 10

Claim 10 recites a computing device comprising:

> a structural parameter configured to indicate a total number of physical ports that are present in the computing system including the one or more front ports and the one or more back ports, the structural parameter being configured to indicate a fewer number of ports than the total number of physical ports in order to prohibit operation of the one or more front ports;

As explained, Thayer teaches enabling an internally hidden port to allow its use. Thayer is not on point. The Office Action cites Figure 1A, item 110 as teaching the claimed structural parameter. Element 110 is a "support logic 110, which may include one or more chips" (Thayer, page 3, [0029]). Thayer makes no other reference to the support logic 110 and provides no other explanation. Therefore, support logic 110 being simply a "chip" fails to teach or suggest any aspect of the claimed structural parameter. Claim 10 is not anticipated for at least this reason and the rejection should be reversed.

Claim 10 also recites: "the structural parameter causing the one or more front ports to be undetectable by the operating system causing the one or more front ports to be inoperable." Conversely, Thayer teaches enabling a port to be used. Thayer fails to anticipate this element and fails to establish a prima facie rejection. The rejection should be reversed.

Independent Claim 16

Claim 16 was rejected merely by reference to the rationale of claim 1 (Final Office Action, page 3). However, claim 16 is a method that recites different

elements than claim 1. Thus, claim 16 has not been addressed by the Office Action and no references to Thayer have been cited as teaching each and every claimed element. Thus a prima facie anticipation rejection of claim 16 has not been established and the rejection cannot stand for at least this reason.

Looking to claim 16, it recites a method for securing a port in a device. As explained, Thayer is directed to enabling and using a hidden port, not securing a port (Thayer, page 2, [0015] lines 1-9). Thus Thayer is not relevant to claim 16 and does not anticipate the claim. Furthermore, claim 16 recites:

> receiving a signal that indicates a number of ports to be secured from user access;

No reference to Thayer has been provided for teaching this element. Indeed, Thayer fails to teach this element. Thayer teaches enabling the use of a port, and not anything related to securing ports from user access.

Claim 16 further recites:

> accessing a data store that contains a value for the total number of physical ports;

No reference to Thayer has been provided for teaching this element. Indeed, Thayer fails to teach this element. The claim is not anticipated.

Lastly, claim 16 recites:

> reducing the value in the data store by the number of ports to be secured to cause an operating system to be aware of a number of physical ports that is less than the total number of physical ports.

The Office Action (page 3) cites Thayer paragraphs [0057-0061] as allegedly teaching changing a port count. As explained under claim 1 above, the

cited paragraphs fail to teach anything related to changing a port count or reducing a value for the total number of ports. The reliance on Thayer is misplaced and Thayer fails to anticipate any feature of claim 16.

A prima facie anticipation rejection has not been established and the rejection should be reversed. Accordingly, the rejections of dependent claims 17-20 are also improper and should be reversed.

Independent Claims 21, 25, and 27

Claims 21, 25 and 27 were rejected in a conclusory manner using the rationale applied to claim 1. As explained, the reliance on Thayer by the Office Action is incorrect and misplaced. The defects of Thayer have been discussed. Thayer fails to anticipate each and every element of claim 21, 25, or 27. Thus a prima facie anticipation rejection has not been established and the rejection should be reversed.

Independent Claim 21

Based on the explanation of Thayer, Thayer fails to teach anything related to "specifying a reduced number of physical ports," "changing a configuration parameter that indicates, to an operating system, the actual number physical ports...", or "causing the operating system not to enumerate the one or more ports" as recited in claim 21. Thayer fails to establish a prima facie anticipation rejection and the rejection should be reversed. Claim 21 and dependent claims 22-24 should now be allowed.

Independent Claim 25

In view of the discussion above, Thayer fails to teach any means for causing an operating system to not enumerate a selected port. Thayer teaches enabling a hidden port to be used. Thayer fails to teach or suggest ways to cause an

operating system to not enumerate a port, thus Thayer fails to anticipate this feature.

Claim 25 also recites that the security means modifies a port count to specify one less port than a total number of the set of physical ports. None of the cited sections of Thayer teach this feature. A prima facie anticipation rejection has not been established for this additional reason. The rejection should be reversed and claim 25 and dependent claim 26 should now be allowed.

Independent Claim 27

Claim 27 was rejected with the same rationale and citations of Thayer as applied against claim 1 (Office Action page 3). However, claim 27 recites different elements from claim 1 and the specific elements from claim 27 were not addressed. Therefore the rationale applied against claim 1 is insufficient for claim 27. Thayer fails to anticipate claim 27.

For example, claim 27 recites:

> "in response to the data entry selection signal ... the configuration parameter stores a value that specifies a total number of physical ports that are present in the computer system, the operation causing the value to be reduced in response to the security status for a selected port being set to indicate a secured status to cause an operating system not to enumerate the selected port.

The cited sections of Thayer fail to discuss anything related to not enumerating a port. Thayer does not discuss reducing a configuration value that specifies a total number of ports and does not discuss anything related to causing an operating system not to enumerate a port. A prima facie anticipation rejection has not been established. The rejection should be reversed and claim 27 should be allowed.

III. Whether claims 4, 8, 13-14, 19, 24, 29-30 are unpatentable under 35 U.S.C. §103(a) as being obvious over Thayer, in view of Zimmer et al. (US Patent Publication 2005/0010811).

Zimmer Figure 8, items 442, 436, and 434 were cited by the Office Action on page 5 against claims 4, 8, 13-14, 19, 24, 29-30. Zimmer fails to discuss Figure 8 or its components in the specification. Figure 8 is not referenced in the "Brief Description of the Drawings" section on page 1 and no accompanying text is disclosed. Rather, the specification of Zimmer ends with Figure 6.

Therefore, figure 8 only teaches an illustrated set of boxes, none of which teach or suggest the claimed elements. Zimmer fails to cure the deficiencies of Thayer and fails to establish a prima facie obviousness rejection when combined. The rejection should be reversed.

The Office Action also cites Zimmer [0022]. Paragraph [0022] discloses that System Management Mode (SMM) code is hidden from an operating system:

> [0022] ... SMM has been available on IA32 (Intel Architecture 32 bit) processors as an operation mode hidden to operating systems that executes code loaded by BIOS or firmware. SMM is a special-purpose operating mode provided for handling system-wide functions like power management, system hardware control, or proprietary OEM-designed code. The mode is deemed "hidden" because the operating system (OS) and software applications cannot see it, or even access it.

A System Management Mode that is hidden to an operating system has no relevance to systems and methods of securing ports as in the present application. For example, hidden SMM code fails to teach or suggest reducing a number in a controller field to cause an operating system to be unaware of one or more companion controllers as in present claim 4. Thus, Zimmer is unrelated to the

present application, fails to teach or suggest the claimed elements, and fails to cure the deficiencies of Thayer.

The combined references fail to establish a prima facie obviousness rejection and the rejection should be reversed. Claims 4, 8, 13-14, 19, 24, 29-30 patentably distinguish over the references of record and should be allowed.

Conclusion

For the reasons set forth above, a prima facie anticipation or obviousness rejection has not been established for any claim. All rejections have been shown to be improper. Appellant respectfully believes that all pending claims 1-30 patentably and unobviously distinguish over the references of record and that the rejections should be withdrawn. Appellant respectfully requests that the Board of Appeals overturn the Examiner's rejections and allow all pending claims. An early allowance of all claims is earnestly solicited.

Respectfully submitted,

SEPT. 2, 2008

Date

Peter Kraguljac (Reg. No. 38,520)

(216) 503-5500
Kraguljac & Kalnay, LLC
Summit One, Suite 510
4700 Rockside Road.
Independence, OH 44131

8. Claims Appendix

1. A system for securing one or more ports of a computing device that includes an actual number of physical ports and a data store that contains a port count specifying the actual number of physical ports, the system comprising:

a configuration logic configured to provide a security option for securing one or more selected ports; and

a security logic configured to, in response to the security option being selected, cause the data store to be modified by changing the port count to specify a fewer number of physical ports to cause an operating system to not detect the one or more selected ports.

2. The system of claim 1 where the security logic is configured to access the data store that includes a register configured to store host controller structural parameters based on an enhanced host controller interface specification.

3. The system of claim 2 where the port count is an N_PORTS field included within the host controller structural parameters that specifies a number of physical ports present in the computing device, the security logic being configured to cause the N_PORTS field to be modified in order to hide the one or more selected ports from the operating system.

4. The system of claim 2 where the host controller structural parameters include a companion controller field that indicates a number of companion controllers associated with the ports, the security logic being configured to cause the companion controller field to be reduced by a number to cause the operating system to be unaware of one or more of the companion controllers.

5. The system of claim 1 where the data store includes a register configured to be read by the operating system during an enumeration process to determine the number of physical ports to enumerate, where the one or more selected ports are not enumerated by the operating system.

6. The system of claim 5 where the number of physical ports indicated in the data store cause the operating system to enumerate a fewer number of ports than the actual number of physical ports.

7. The system of claim 1 where the system configuration logic includes a graphical user interface.

8. The system of claim 1 where the system is embodied as a computer-readable medium configured to provide the system configuration logic and the security logic as processor executable instructions.

9. The system of claim 1 where the one or more selected ports are front ports of the computing device.

10. A computing system, comprising:

a housing;

one or more processors;

a set of physical ports including:

one or more front ports positioned on the housing and being accessible by a user to connect an external device to the computing system; and

one or more back ports, positioned on the housing, being configured to connect an external device to the computing system;

a structural parameter configured to indicate a total number of physical ports that are present in the computing system including the one or more front ports and the one or more back ports, the structural parameter being configured to indicate a fewer number of ports than the total number of physical ports in order to prohibit operation of the one or more front ports; and

an operating system configured to enumerate ports that are present in the computing system based on the structural parameter, the structural

parameter causing the one or more front ports to be undetectable by the operating system causing the one or more front ports to be inoperable.

11. The computing system of claim 10 where the fewer number of ports indicated in the structural parameter causes the operating system to not enumerate the one or more front ports so that no operable connection is established between the one or more front ports and the operating system.

12. The computing system of claim 10 where the one or more front ports are logically numbered with greater port numbers than the one or more back ports, and where the operating system is configured to enumerate ports from a lowest to highest port number.

13. The computing system of claim 10 where the structural parameter is a data stored configured to contain a plurality of configuration parameters.

14. The computing system of claim 10 where the set of physical ports are universal serial bus (USB) ports and where the computing system further includes:

a high speed host controller configured to control selected ports of the set of physical ports at a first communication speed;

one or more companion controllers configured to control selected ports of the set of physical ports at one or more communication speeds that are different than the first communication speed; and

a companion controller field configured to specify a number of actual companion controllers where the companion controller field being modified to specify a fewer number of companion controllers than the number of actual companion controllers to account for the one or more front ports being undetected by the operating system.

15. The computing system of claim 10 further including:

a graphical user interface configured to allow a user to select the one or more front ports to be inoperable or operable; and

a port security logic configured to reconfigure the structural parameter to modify the total number of physical ports stored therein in response to the one or more front ports being selected to be inoperable or operable.

16. A method for securing a port in a device having a total number of physical ports, the method comprising:

receiving a signal that indicates a number of ports to be secured from user access;

accessing a data store that contains a value for the total number of physical ports; and

reducing the value in the data store by the number of ports to be secured to cause an operating system to be aware of a number of physical ports that is less than the total number of physical ports.

17. The method of claim 16 further including:

providing an option to a user to secure a port; and

in response to the option being selected, generating the signal that indicates the number of ports to be secured.

18. The method of claim 16 where the total number of physical ports include one or more front ports positioned on the device and being accessible by a user, and one or more back ports positioned on the housing, and where the signal indicates to secure the one or more front ports; and

where the reducing step includes reducing the value by the number of the one more front ports to cause the operating system to not enumerate the one or more front ports.

19. The method of claim 18 further including:

storing a controller value that specifies a number of controllers present in the device that are configured to control the physical ports; and

reducing the controller value by a number of controllers that are associated with the one or more front ports to cause the operating system to not enumerate the controllers that are associated with the one or more front ports.

20. The method of claim 18 where the reducing step includes:

enabling the data store to be writeable;

modifying the value in the data store to specify the number of physical ports that is less than the total number of physical ports; and

enabling the data store to be read-only.

21. A computer-readable medium for providing processor executable instructions operable to perform a method, the method comprising:

providing a security option to secure one or more ports of a device;

in response to the security option being selected for a port, specifying a reduced number of physical ports that is less than an actual number of physical ports present in the device; and

changing a configuration parameter that indicates, to an operating system, the actual number physical ports, where the configuration parameter is changed to indicate the reduced number of physical ports causing the operating system not to enumerate the one or more ports.

22. The computer-readable medium of claim 21 where changing the configuration parameter to the reduced number of physical ports causes no operable connection to be established between the one or more ports and the operating system.

23. The computer-readable medium of claim 21 further including processor executable instructions to cause a processor to:

enable the configuration parameter to be writeable;

change the configuration parameter to indicate the reduced number of physical ports; and

enabling the configuration parameter to be read-only.

24. The computer-readable medium of claim 21 where the configuration parameter includes a host controller structural parameter associated with a universal serial bus controller.

25. A system, comprising:

port configuration means for selecting a port to be secured from a set of physical ports configured within a computing device; and

security means for causing an operating system to not enumerate the selected port to cause the selected port to be inoperable, including modifying a port count to specify one less port than a total number of the set of physical ports where the operating system enumerates ports based on the port count.

26. The system of claim 25 where the security means is further configured to modify the port count by one or more values.

27. In a computer system having a graphical user interface comprising a display and a selection device, a method of providing and selecting from a set of data entries on the display, the method comprising:

retrieving a one or more data entries, where a data entry represents a security status of a port;

displaying the one or more data entries on the display to show the security status and allow the security status to be modified;

receiving a data entry selection signal indicative of the selection device selecting one or more of the data entries that modifies the security status of a port; and

in response to the data entry selection signal, initiating an operation that causes a configuration parameter to be modified in accordance with the security status where the configuration parameter stores a value that specifies a total number of physical ports that are present in the computer system, the operation causing the value to be reduced in response to the security status for a selected port being set to indicate a secured status to cause an operating system not to enumerate the selected port.

28. The graphical user interface of claim 27 where the security status includes an available status and a hidden status.

29. The graphical user interface of claim 27 where the configuration parameter is configured as part of a host controller structural parameter associated with a host controller that provides an interface to one or more ports in the computer system.

30. The graphical user interface of claim 29 where the one or more ports are universal serial ports.

9. Evidence Appendix

None. There is no extrinsic evidence.

10. Related Proceedings Appendix

None. There are no related proceedings.